Achieving ISO 27001 Certification

26th - 27th November 2008

Venue : Sheraton Bahrain Hotel, Manama, Bahrain

Why Attend This?

- Taught by framework author(s) and subject matter experts directly
- OISSG developed US$20,000 worth of tools for free
- Continual online support
- A platform for continuous learning via Local Chapter
- Opportunity to speak to instructors after the course
- 100% satisfaction by attendees, contact us for referals

OISSG
A Non-Profit Organisation
www.oissg.org

- **35% discounted fees**
- **Team Discount: Register 3 delegates and the 4th comes for FREE!**

Cost: US$ 1,000/-PP Only

Venue: Sheraton Bahrain Hotel, Manama, Bahrain
Contact: +971 50 9498488, Fax: +971 4 3985166, Email: registration@oissg.org

Overview

Achieving ISO 27001 Certification Program empowers you to successfully certify your organization against ISO 27001 through a robust security system. Often, mere compliance to a framework may not mean reduced risk for the organization. In order to deliver full advantage of the management system, drill-down level of techniques and tools need to be deployed to ensure complete and effective risk management.

ISO 27001 provides a blueprint for an information security management system (ISMS) based on a risk management approach, to establish, implement, operate, monitor, maintain and improve information security. Besides, certification is an accepted way of providing assurance that the organization has implemented a management system which meets the requirements specified in the ISO 27001 standard.

From on-going field research of renowned security practitioners across the globe, we have narrowed down to a mix of security tools, techniques and knowledge which provide our course participants the most needed and valuable security skills to achieve ISO 27001 certification. Besides, some tools used in this course address the critical success factors and common challenges faced in an information security project.

OISSG

Duration, Business Benefits, Target Audience

DURATION

- This course will be covered in two days.
- Course timings 08:00 to 16:30 with scheduled lunch and refreshment breaks.

MEALS AND REFRESHMENTS:

Daily lunch buffet and refreshments is included in the tuition fees

KEY BUSINESS BENEFITS OF ATTENDING THIS EVENT:

- Achieve 27001 Certification for Your Organization
- Get required tools, templates and resources to achieve certification
- Learn effective ISO 27001 implementation methodologies
- Pre-audit your information security management system
- Effective and detailed management of information risks
- Learn ISO 27001 risk assessment methodologies
- Make strong business case for security spending in your organization

WHO SHOULD ATTEND:

Managers and Professionals who are looking to certify their organizations for ISO 27001 and/or upgrade their skills on ISO 27001 implementation and compliance assessment including:

- IT Managers, IT Auditors, Computer Auditors
- IT Security Officers
- Security Administrator(s), System and Network Administrator(s)
- Information Security Professionals
- Risk Analysts

Laptop Needed

Deliverables

In addition to all the presentation material, following handbooks and tools would be provided to support participants' ability to lead ISMS implementation and certification in their organizations:

1. COURSE MATERIAL

Handbook 1 - Implementation of Mandatory Requirements

Along with a detailed narrative of the certification and audit process, this material gives useful insights on mandatory process requirements and suitable implementation strategies.

Handbook 2 - Gap Analysis Questionnaire

This guide presents each of the control requirements in a question form to help an organization assess:

- If a control requirement has been implemented and evidence can be provided to support this claim or;
- What gaps exist in the current implementation and reasons and justification for the same

Handbook 3 - Implementation and Audit Manual

This document provides guidance on implementation of ISMS control requirements and for auditing existing implementations. It discusses each of the controls in Annex A of ISO 27001 from auditing and implementation viewpoints.

Handbook 4 - How to Measure Effectiveness of your ISMS?

ISO 27001 requires an organization to measure effectiveness of its ISMS implementation. This guide provides information and help on measuring effectiveness of controls implemented as part of ISMS.

2. ISMS IMPLEMENTATION KIT

ISO 27001 Posture Evaluation Framework (IPEF):

ISO 27001 Posture Evaluation Framework (IPEF) provides a dipstick assessment, including a graphical representation, of an organization's current security implementation. This provides quick start to creating or strengthening of existing security system, besides an as is snapshot of the organization.

ISO 27001 Ice-breaker:

ISO 27001 Preliminary Assessment Framework (IPAF) provides a head-start for planning process with scientific method for identification and classification of information assets besides a method for identifying information security objectives, which are aligned with business goals.

Deliverables

ISO 27001 Risk Management Framework (IRMF):
Created from field experience and applied security knowledge of several security experts, this risk management framework:

1. Provides a complete list of most probable and applicable threats collated from different bodies of knowledge;
2. Enables a Security Manager to develop most relevant threat scenarios and
3. Evaluate risk levels to key information assets as function of business impact and likelihood.

Return On Security Investment (ROSI) Calculator:
Information security must minimize business risk and maximize return on investments and business opportunities. This tool provides a focused quantitative assessment of business value against the investment of resources for security.

Security Projects Decisioning Framework (SPDF)
This path-breaking decisioning framework scientifically measures risks mitigated and strategic objectives achieved. This provides for a much needed model for presenting effectual business cases for security projects.

Security Policy Awareness Tool (SPAT)
This tool focuses on effective and auditable distribution of relevant policies to different user groups. It works interactively as a gate-keeper during log-on process to caution a user on key policy aspects, prior to system use. The system keeps a trail of users' interactions for records.

3. VULNERABILITY ASSESSMENT AND PENETRATION TESTING TOOLS

Compiled through field work of several professionals, this unique collection of security tools, on three CD volumes, provides a set of effective, current and tested tools in one place. This makes the most required tools in a given situation readily available, thus saving time and energy for vulnerabilities management.

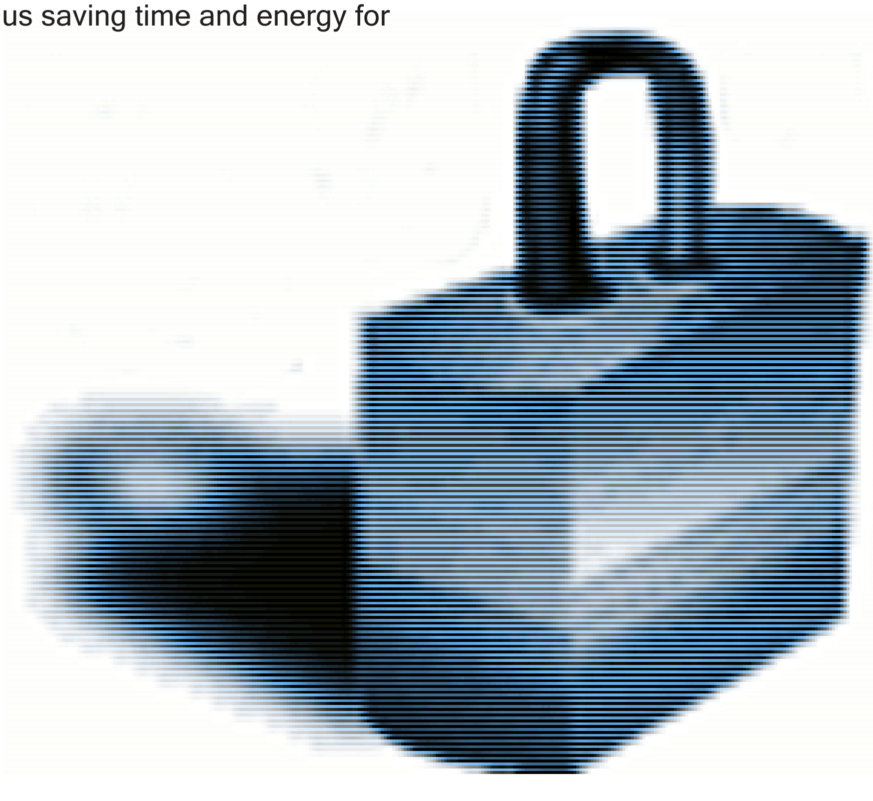
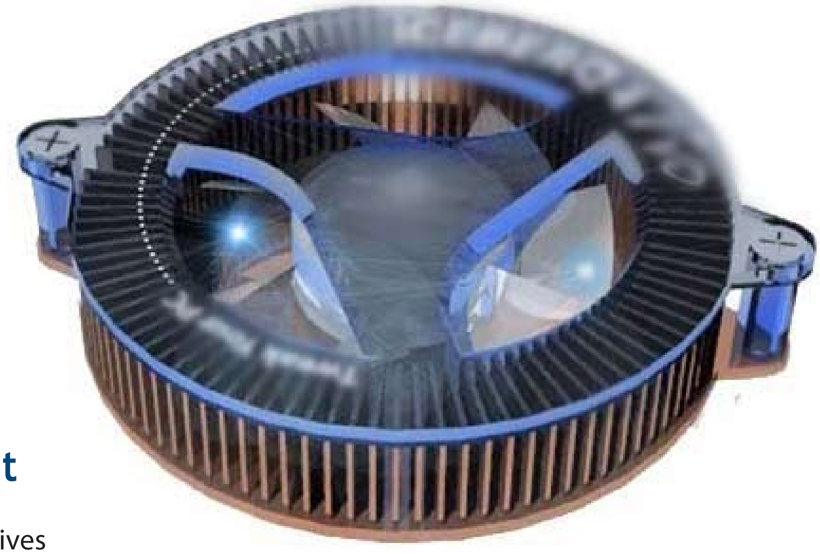


Table of contents

Following modules lead a course participant step-by-step through ISO 27001, from preliminary assessment until a stage of pre-audit before final certification:

- Simplifying Plan-Do-Check-Act Cycle of ISO 27001
- ISO 27001 - Terms and Definitions you must know
- Does it make business sense for my company to go for ISO27001 certification?
- ISO 27001 Survival Kit – what you need to get started?
- Critical Success Factors to Achieving ISO27001 Certification



Exercise 1 – Panel discussion using ISO 27001 Posture Evaluation Framework (IPEF)

PLAN PHASE - Part 1: Preliminary Assessment

- Understanding Business Goals and aligning Security Objectives
- Defining Enterprise Security Objectives
- Define the Scope of ISMS
- Define Top Level Security Policy

Exercise 2 – Define Security Objectives and Top-level Security Policy
Tool used: ISO 27001 Ice-breaker

- Map Processes and Information Flows
- Identifying Information Assets

Exercise 3 – Mapping Information Flow and Asset Identification
Tool used: ISO 27001 Ice-breaker:

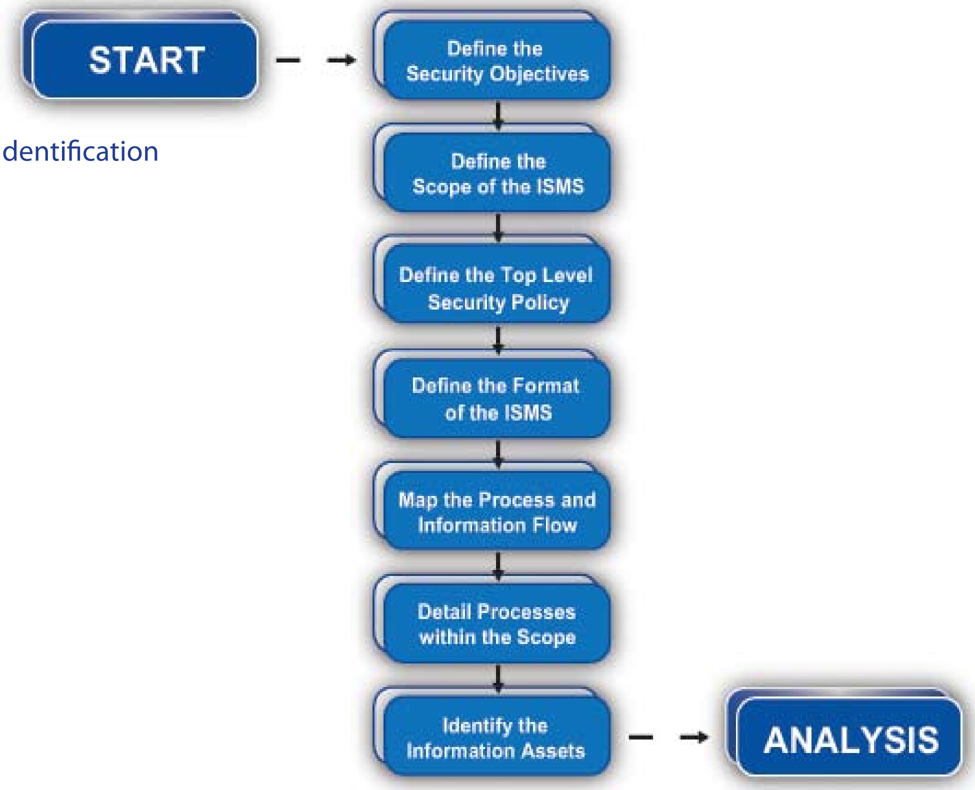
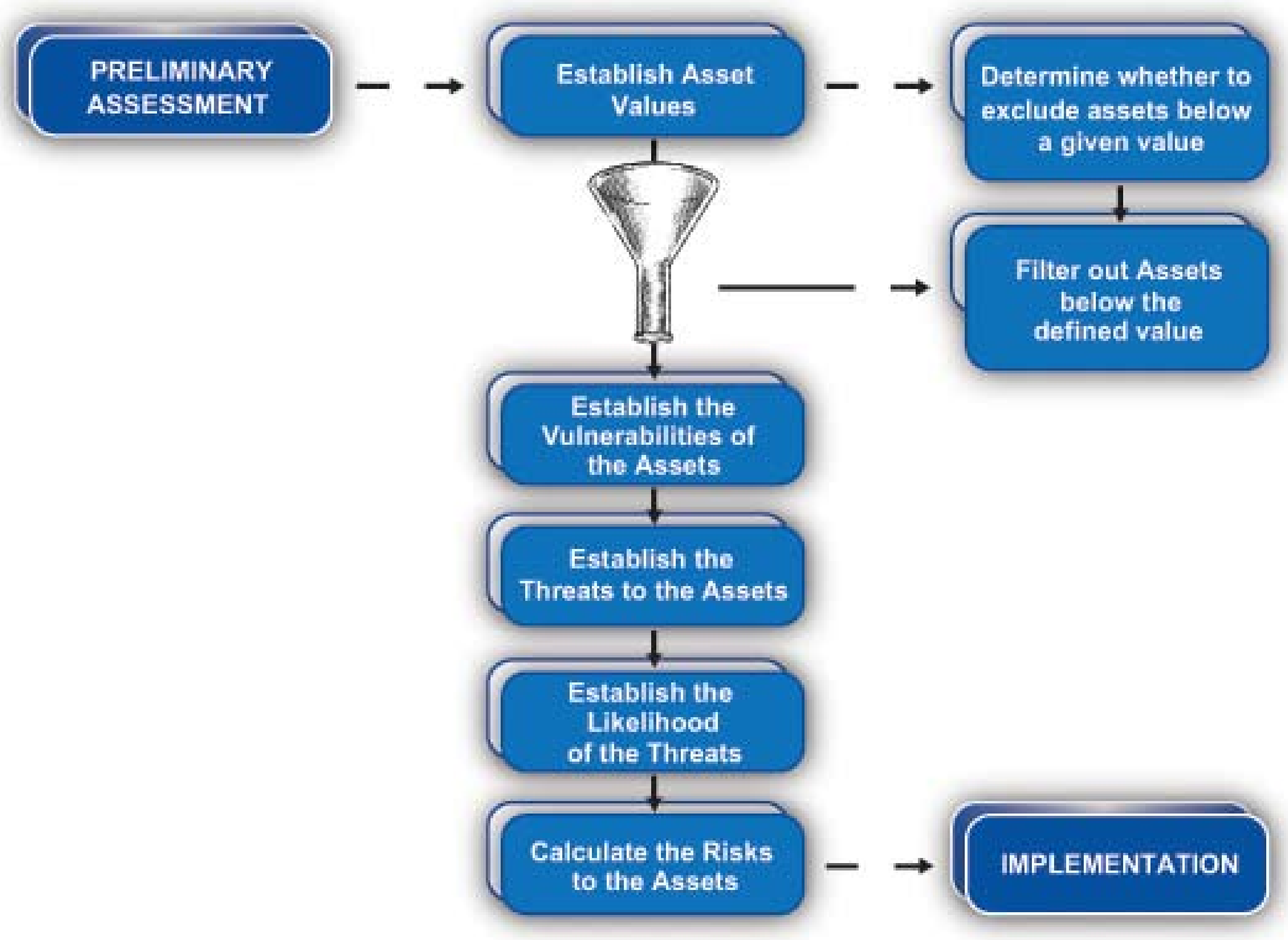

START
Define the Security Objectives
Define the Scope of the ISMS
Define the Top Level Security Policy
Define the Format of the ISMS
Map the Process and Information Flow
Detail Processes within the Scope
Identify the Information Assets
ANALYSIS

TABLE OF CONTENTS...

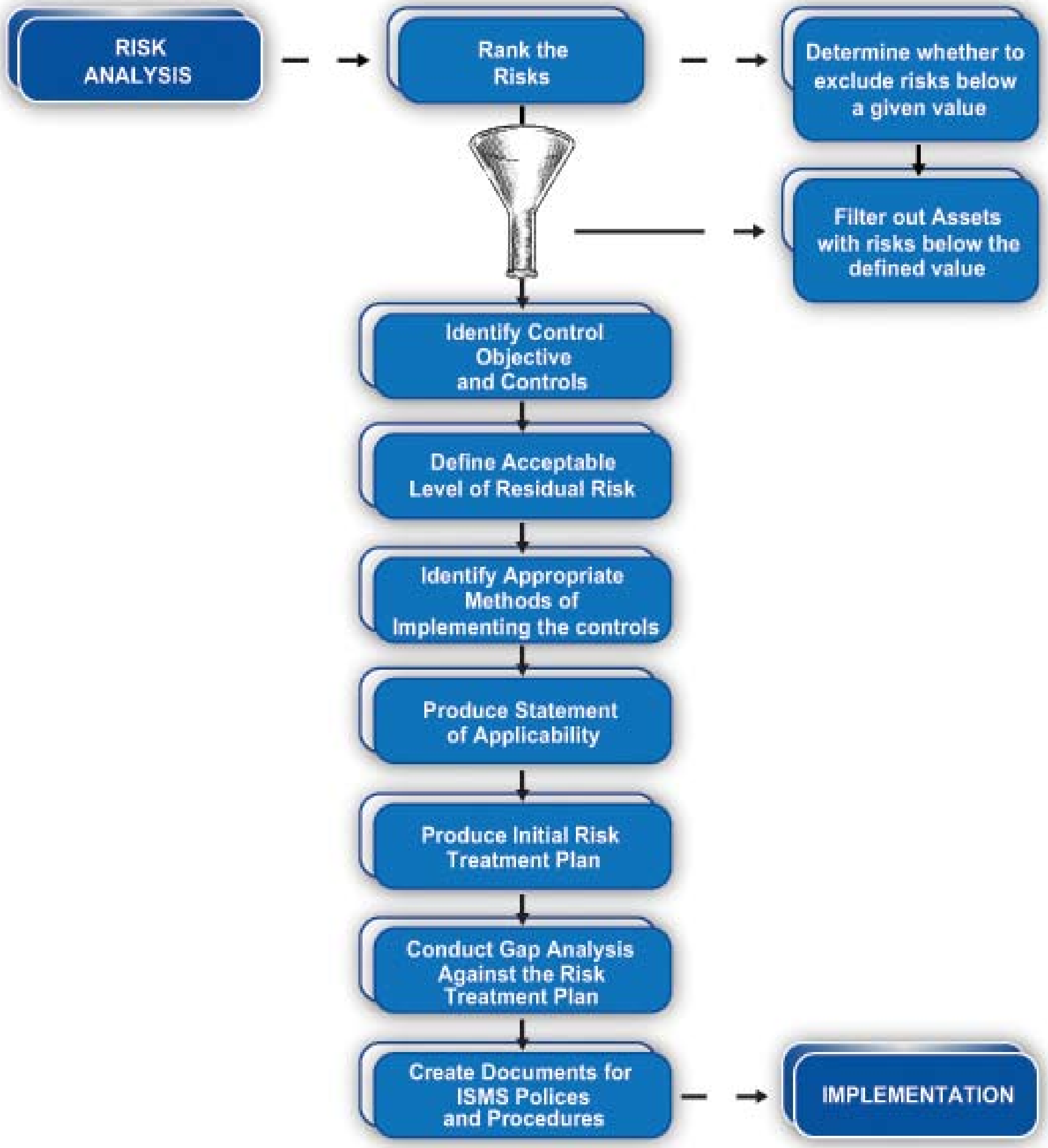
PLAN PHASE - Part 2: Risk Analysis



PRELIMINARY ASSESSMENT
Establish Asset Values
Determine whether to exclude assets below a given value
Filter out Assets below the defined value
Establish the Vulnerabilities of the Assets
Establish the Threats to the Assets
Establish the Likelihood of the Threats
Calculate the Risks to the Assets
IMPLEMENTATION

Table of contents...

PLAN PHASE - Part 3: ISMS Planning and Design



RISK ANALYSIS

Rank the Risks

Determine whether to exclude risks below a given value

Filter out Assets with risks below the defined value

Identify Control Objective and Controls

Define Acceptable Level of Residual Risk

Identify Appropriate Methods of Implementing the controls

Produce Statement of Applicability

Produce Initial Risk Treatment Plan

Conduct Gap Analysis Against the Risk Treatment Plan

Create Documents for ISMS Polices and Procedures

IMPLEMENTATION

Table of contents...

YOUR EXPERT COURSE INSTRUCTOR

PRINCIPAL INSTRUCTOR

Balwant Rathore
Vice President
Open Information Systems Security Group (OISSG)
http://www.oissg.org/

It's rare to find a true industry luminary and innovator teaching a certification boot camp class for budding professionals wanting to broaden their information security skill set. But leader and standard-setter, Balwant Rathore, sees sharing his extensive knowledge and experience with his students as "a privilege and a responsibility.

Balwant Rathore is a visionary entrepreneur and an avid information security professional. This time he is into the invention of Information Systems Security Assessment Framework (ISSAF) along with team OISSG which comprises of a globally recognized team of information security professionals. Prior to this, Balwant had an outstanding and award winning performance in an acclaimed police organization.

Balwant has provided security assessments, business continuity and computer crime investigation services to a wide variety of banking and financial institutions, including several "Top 10" banks, Telecom sector and many more multinational companies and government enterprises in Europe, North America, and Asia. Balwant is a technologist and frequently invited speaker to security briefings and corporate information security conferences across the globe. His articles are also printed in magazines such as InformIT, Voice&Data, Network Magazines etc.

Under his leadership as the founding member of OISSG and current Vice President, OISSG has emerged from a think tank of IT Security professionals to a professionally managed organization. In his spare time, he develops new methodologies, security tools, and contributes to open source security projects.

About OISSG

Open Information Systems Security Group (OISSG) is a not-for-profit organization head quartered in London. Our vision is to spread information security awareness by hosting an environment where security enthusiasts from all over the globe share and build knowledge. It was established with the objective of evolving a set of open standards, guidelines and good practices in the area of information security. As a first step in this direction, a comprehensive framework for the assessment of information systems security has been released. The Framework is known as ISSAF, which can be downloaded from www.oissg.org/issaf.

1920 Ambleside dr.
Colorado Springs
Colorado, USA 80915
Phone: +1 719 573 4949
Fax: +1 719 573 4950
Email: info.us@oissg.org
Web: www.oissg.org

2nd Floor, 145-157 St. John Street,
London, EC1V 4PY,
United Kingdom.
Phone : +44 (0) 207 871 4033
Fax : +44 (0) 207 160 5209
Email : info.uk@oissg.org
Web : www.oissg.org

Registration Form

Event: Achieving ISO 27001 Certification, Bahrain

Delegate 1: Title _____ First Name _________________________ Surname ___________________
Job Position _________________________ Email: ____________________ Tel: ________________

Delegate 2: Title _____ First Name _________________________ Surname ___________________
Job Position _________________________ Email: ____________________ Tel: ________________

Delegate 3: Title _____ First Name _________________________ Surname ___________________
Job Position _________________________ Email ____________________ Tel: ________________

Delegate 4: Title _____ First Name _________________________ Surname ___________________
Job Position _________________________ Email ____________________ Tel: ________________

REMEMBER EVERY 4TH DELEGATE GOES FREE

To assist us with future correspondence, please supply the following information if applicable:

Head of Department Name ___________________________ Email: ____________________ Tel:_____________________

Training Manager Name____________________________ Email ____________________ Tel:_____________________

Administrative (Booking) Contact Name ____
Email: ________________________________ Tel_____________________

Cancellation policy
In the event you are unable to attend this training a replacement delegate may be sent in your place. Should you wish to cancel your registration we will refund your registration fee less an administration cost of $ 200 per registered delegate. We also reserve the right to cancel or postpone this training where full refunds will be issued.

Privacy Act notice
OISSG Trainings are promoted by a number of supporting organisations' that may send you this brochure on our behalf. If you do not wish to receive further mailing from OISSG, please tick the box below and return to us at P.O.Box 31303, Dubai, UAE or Fax back to +971 4 3985166.
We will then remove your details from any of our mailing lists.

□ Please do not mail me further brochures regarding your trainings

Register Now
Contact Marketing at OISSG
Tel :+971 50 9498488
Fax : +971 4 3985166
Email : registration@oissg.org

OISSG

A Non-Profit
Organisation
www.oissg.org

Workshop : 26th - 27th November (2 Days)
Time : 08:00 - 16:30

- **35% discounted fees**
- **Team Discount: Register 3 delegates and the 4th comes for FREE!**

Cost: US$ 1,000/-Per Person Only

Venue: Sheraton Bahrain Hotel, Manama, Bahrain
Contact: +971 50 9498488, Fax: +971 4 3985166, Email: registration@oissg.org